What is claimed is:

1. A machine-implemented method comprising:

receiving requests for network communication services from an invoked application;

selectively designating each of the received requests as authorized or unauthorized based on an application-specific network policy; and

monitoring inbound network communications, based on the authorized requests, to detect an intrusion.

2. The method of claim 1, wherein monitoring inbound network communications comprises:

blocking the inbound network communications that fail to correspond to an authorized request; and

monitoring the blocked inbound network communications to detect an intrusion.

3. The method of claim 2, wherein monitoring the blocked inbound network communications comprises:

examining the blocked inbound network communications to detect an intrusion prelude;

identifying a source for a detected intrusion prelude; and

initiating monitoring of inbound network communications from the identified source.

4. The method of claim 3, wherein examining the blocked inbound network communications comprises checking for patterns spanning multiple communications.

5. The method of claim 4, wherein monitoring the blocked inbound network communications further comprises generating fabricated responses to the blocked inbound network communications.

6. The method of claim 3, wherein the monitoring of inbound network communications from the identified source comprises checking the inbound network communications from the identified source for packet-level exploits.

7. The method of claim 1, further comprising increasing a monitoring level for network communications for the invoked application in response to one or more unauthorized requests.

8. The method of claim 7, wherein increasing a monitoring level for network communications for the invoked application comprises initiating monitoring of the network communications for the invoked application using an application-specific intrusion signature.

9. The method of claim 8, further comprising identifying the invoked application by examining a set of instructions embodying the invoked application.

10. The method of claim 9, wherein monitoring of the network communications for the invoked application comprises monitoring in an intrusion detection system component invoked with the invoked application.

11. The method of claim 10, wherein the intrusion detection system component and the invoked application run within a single execution context.

12. The method of claim 9, wherein examining the set of instructions comprises:

applying a hash function to the set of instructions to generate a condensed representation; and

comparing the condensed representation with existing condensed representations for known applications.

13. A machine-implemented method comprising:

identifying an invoked application;

receiving requests for network communication services from the invoked application;

selectively designating each of the received requests as authorized or unauthorized based on an application-specific network policy;

blocking inbound network communications that fail to correspond to an authorized request;

monitoring the blocked inbound network communications to detect an intrusion; and

initiating monitoring of network communications for the invoked application using an application-specific intrusion signature in response to one or more unauthorized requests.

14. The method of claim 13, wherein monitoring the blocked inbound network communications comprises:

examining the blocked inbound network communications to detect an intrusion prelude;

identifying a source for a detected intrusion prelude; and

initiating monitoring of inbound network communications from the identified source.

15. The method of claim 14, wherein identifying the invoked application comprises examining a set of instructions embodying the invoked application.

16. The method of claim 15, wherein examining the

blocked inbound network communications comprises checking for patterns spanning multiple communication.

17. The method of claim 16, wherein monitoring the blocked inbound network communications further comprises generating fabricated responses to the blocked inbound network communications.

18. The method of claim 15, wherein monitoring of inbound network communications from the identified source comprises checking the inbound network communications from the identified source for packet-level exploits.

19. The method of claim 18, wherein examining the set of instructions comprises:

applying a hash function to the set of instructions to generate a condensed representation; and

comparing the condensed representation with existing condensed representations for known applications.

20. The method of claim 19, wherein monitoring of the network communications for the invoked application comprises monitoring in an intrusion detection system component invoked with the invoked application.

21. The method of claim 20, wherein the intrusion detection system component and the invoked application run within a single execution context.

22. A system comprising:

an application network policy enforcer, which services network requests from an application invoked on a machine, identifies the network requests that fail to satisfy an application-specific network policy, and identifies the network requests that satisfy the application-specific network policy;

a network traffic enforcer, which blocks inbound network traffic that does not correspond to the network requests identified by the application network policy enforcer as satisfying the application-specific network policy; and

an intrusion detector, which responds to the network requests identified by the application network policy enforcer as failing to satisfy the application-specific network policy, and which responds to the inbound network traffic blocked by the network traffic enforcer.

23. The system of claim 22, wherein the intrusion detector comprises:

a first component that responds to the network requests

identified as failing to satisfy the application-specific network policy by monitoring traffic for the invoked application, wherein the first component shares a software module with the application network policy enforcer; and

a second component that responds to the blocked traffic by monitoring traffic for an identified source of an intrusion prelude detected in the blocked traffic, wherein the second component shares a software module with the network traffic enforcer.

24. A system comprising:

means for servicing network requests from an application invoked on a machine;

means for authorizing the network requests using an application-specific network policy;

means for blocking traffic that does not correspond to an authorized request;

means for monitoring blocked traffic to identify an intrusion prelude and to identify abnormal application behavior;

means for detecting an intrusion in response to an identified intrusion prelude; and

means for detecting an intrusion in response to identified abnormal application behavior.

25. The system of claim 24, wherein the means for detecting an intrusion in response to an identified intrusion prelude comprises means for detecting packet-level exploits for traffic from an identified source of the identified intrusion prelude, and wherein the means for detecting an intrusion in response to identified abnormal application behavior comprises means for detecting application-specific intrusion signatures for traffic corresponding to an abnormally behaving application, the system further comprising:

means for generating a fabricated response to blocked traffic to gain knowledge about a potential intruder; and

means for responding to a detected intrusion.

26. A machine-readable medium embodying machine instructions for causing one or more machines to perform operations comprising:

identifying an invoked application;

receiving requests for network communication services from the invoked application;

selectively designating each of the received requests as authorized or unauthorized based on an application-specific network policy;

blocking inbound network communications that fail to correspond to an authorized request;

monitoring the blocked inbound network communications to detect an intrusion; and

initiating monitoring of network communications for the invoked application using an application-specific intrusion signature in response to one or more unauthorized requests.

27. The machine-readable medium of claim 26, wherein monitoring the blocked inbound network communications comprises:

examining the blocked inbound network communications to detect an intrusion prelude;

identifying a source for a detected intrusion prelude; and

initiating monitoring of inbound network communications from the identified source.

28. The machine-readable medium of claim 27, wherein identifying the invoked application comprises examining a set of instructions embodying the invoked application.

29. The machine-readable medium of claim 28, wherein monitoring of inbound network communications from the identified source comprises checking the inbound network communications from the identified source for packet-level exploits.

30. The machine-readable medium of claim 29, wherein examining the set of instructions comprises:

applying a hash function to the set of instructions to generate a condensed representation; and

comparing the condensed representation with existing condensed representations for known applications.

31. A machine-implemented method comprising:

blocking inbound network communications that fail to correspond to a network policy;

detecting a potential intrusion prelude from the blocked inbound network communications;

selectively generating a fabricated response to the detected potential intrusion prelude; and

receiving information about a potential intruder in response to the generated fabricated response.

32. The method of claim 31, wherein the network policy comprises an application-specific network policy, the method further comprising:

receiving requests for network communication services from an invoked application;

selectively designating each of the received requests as authorized or unauthorized based on the application-

specific network policy;

monitoring the blocked inbound network communications to detect an intrusion; and

associating the information about the potential intruder with a detected intrusion.

33. The method of claim 32, wherein monitoring the blocked inbound network communications comprises:

examining the blocked inbound network communications to detect an intrusion prelude;

identifying a source for a detected intrusion prelude; and

initiating monitoring of inbound network communications from the identified source.